

**IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION**

KONNECH, INC.,

PLAINTIFF,

v.

**TRUE THE VOTE, INC., GREGG
PHILLIPS, and CATHERINE
ENGELBRECHT,**

DEFENDANTS.

§
§
§
§
§
§
§
§
§
§
§

CIVIL ACTION NO. 4:22-CV-03096

**PLAINTIFF KONNECH, INC.'S RESPONSE TO DEFENDANTS' MOTION TO
DISSOLVE PRELIMINARY INJUNCTION**

KASOWITZ BENSON TORRES LLP

Constantine Z. Pamphilis
Attorney in Charge
Texas State Bar No. 00794419
SDTX Bar No. 19378
DPamphilis@kasowitz.com
Nathan W. Richardson
Texas State Bar No. 24094914
SDTX Bar No. 24094914
NRichardson@kasowitz.com
1415 Louisiana Street, Suite 2100
Houston, Texas 77002
(713) 220-8800
(713) 222-0843 (fax)

Attorneys for Plaintiff Konnech, Inc.

TABLE OF CONTENTS

| | |
|---|-----|
| TABLE OF CONTENTS..... | ii |
| TABLE OF AUTHORITIES | iii |
| PRELIMINARY STATEMENT | 1 |
| BACKGROUND | 3 |
| ARGUMENT | 7 |
| A. Defendants Have Not Identified Any Significant Change of Fact or Law | 7 |
| B. Defendants Produced No Evidence To Support Dissolving the Preliminary Injunction.... | 9 |
| C. The Preliminary Injunction is Valid and Should Not Be Dissolved | 10 |
| 1. Konnech Demonstrated a Substantial Likelihood of Success on the Merits | 12 |
| i. Defendants Publicly Claimed to Hacking Konnech’s Computers | 12 |
| ii. Using a Password Without Authorization to Access a Computer Constitutes Hacking | 18 |
| 2. Konnech Demonstrated Threats of Immediate and Irreparable Harm..... | 21 |
| 3. Konnech Demonstrated that the Balance of Hardships Weighs in Konnech’s Favor .. | 23 |
| 4. Konnech Demonstrated that the Preliminary Injunction is in the Public’s Interest..... | 25 |
| PRAYER..... | 26 |

TABLE OF AUTHORITIES

| | Page(s) |
|--|---------------|
| Cases | |
| <i>Ahmad v. City of St. Louis</i> , 995 F.3d 635 (8th Cir. 2021) | 7, 9 |
| <i>Alto v. Black</i> , 738 F.3d 1111 (9th Cir. 2013) | 8 |
| <i>Bear Ranch, L.L.C. v. Heartbrand Beef, Inc.</i> , 885 F.3d 794 (5th Cir. 2018) | 7 |
| <i>Enargy Power Co. v. Xiaolong Wang</i> , No. 13-11348-DJC, 2013 WL 6234625 (D. Mass. Dec. 3, 2013) | 21 |
| <i>Facebook, Inc. v. Power Ventures, Inc.</i> , 252 F. Supp. 3d 765 (N.D. Cal. 2017), <i>aff'd</i> , 749 F. App'x 557 (9th Cir. 2019) | 21, 25 |
| <i>Favia v. Indiana Univ. of Penn.</i> , 7 F.3d 332 (3d Cir. 1993)..... | 7, 8 |
| <i>Fiber Sys. Int'l, Inc. v. Applied Optical Sys., Inc.</i> , No. 2:06-CV-473, 2009 WL 8590962 (E.D. Tex. June 24, 2009) | 9 |
| <i>Fletcher's Original State Fair Corny Dogs, LLC v. Fletcher-Warner Holdings LLC</i> , 434 F. Supp. 3d 473 (E.D. Tex. 2020)..... | 22 |
| <i>Florida Atlantic Univ. Bd. of Trustees v. Parsont</i> , 465 F. Supp. 3d 1279 (S.D. Fla. 2020) | <i>passim</i> |
| <i>Fox v. City of West Palm Beach</i> , 383 F.2d 189 (5th Cir. 1967) | 24 |
| <i>Franklin Twp. V. Sewerage Auth. V. Middlesex Cnty. v. Utilities Auth.</i> , 787 F.2d 117 (3d Cir. 1986)..... | 8 |
| <i>Heil Trailer Int'l, Co. v. Kula</i> , No. 4:12-cv-385-Y, 2012 WL 12877645 (N.D. Tex. Aug. 21, 2012) | 11 |
| <i>HiQ Labs, Inc. v. LinkedIn Corp.</i> , 31 F.4th 1180 (9th Cir. 2022) | 16, 19, 20 |
| <i>Horne v. Flores</i> , 557 U.S. 433 (2009)..... | 7 |

| | |
|---|---------------|
| <i>ICEE Distributors, Inc. v. J&J Snack Foods Corp.</i> , 445 F.3d 841 (5th Cir. 2006) | 7 |
| <i>Karnoski v. Trump</i> , 926 F.3d 1180 (9th Cir. 2019) | 8 |
| <i>Lamb v. Millennium Challenge Corp.</i> , 334 F. Supp. 3d 204 (D. D.C. 2018) | 22 |
| <i>Lichtenberg v. Besicorp Grp. Inc.</i> , 204 F.3d 397 (2d Cir. 2000)..... | 8 |
| <i>Mach 1, LLC v. Adaptisoft, LLC</i> , No. SA-21-CV-00114-XR, 2021 WL 6750834 (W.D. Tex. Feb. 16, 2021) | 22 |
| <i>MediaOne of Delaware, Inc. v. E & A Beepers & Cellulares</i> , 43 F. Supp. 2d 1348 (S.D. Fla. 1998) | 23 |
| <i>MILLC v. Fpusa, LLC</i> , No. SA:15-CV-406-DAE, 2016 WL 6088344 (W.D. Tex. Oct. 17, 2016) | 7 |
| <i>Quantab Techs. Ltd. v. Golevsky</i> , 719 F. Supp. 2d 766 (S.D. Tex. 2010) | 10 |
| <i>Reliable Prop. Servs., LLC v. Capital Growth Partners, LLC</i> , 1 F. Supp. 3d 961 (D. Minn. 2014)..... | 21 |
| <i>Total Safety v. Knox</i> , 4:19-CV-02719. 2019 WL 6894683 (S.D. Tex. Dec. 18, 2019)..... | 7, 9 |
| <i>U.S. Dept. of Defense v. Federal Labor Relations Authority</i> , 510 U.S. 487 (1994)..... | 22 |
| <i>U.S. v. Nosal II</i> , 844 F.3d 1024, 1038 (9th Cir. 2016) | 19 |
| <i>United States v. Swift & Co.</i> , 286 U.S. 106 (1932)..... | 9 |
| <i>Van Buren v. United States</i> , 141 S. Ct. 1648 (2021)..... | 20 |
| <i>YourNetDating, Inc. v. Mitchell</i> , 88 F. Supp. 2d 870 (N.D. Ill. 2000) | 23 |
| Statutes | |
| 18 U.S.C. § 1030..... | <i>passim</i> |

| | |
|---|---------|
| 28 U.S.C. § 1292(a)(1)..... | 1, 5, 8 |
| TEX. BUS. & COMM. CODE § 521 | 22 |
| Tex. Civ. Prac. & Rem. Code § 143.001 | 3, 10 |

Rules

| | |
|---------------------------------|-------|
| FED. R. APP. P. 4(a)(1)(A)..... | 5 |
| FED. R. CIV. P. 12(b)(6) | 5, 11 |
| Fed. R. Civ. P. 59(e) | 8 |
| FED. R. CIV. P. 60(b)(5)..... | 7 |

Plaintiff Konnech, Inc. (“Konnech”) files this Response in Opposition to Defendants’ Motion to Dissolve Preliminary Injunction (“Motion to Dissolve”) based on the following grounds:

PRELIMINARY STATEMENT

Defendants’ Motion to Dissolve, which is virtually identical to their mandamus brief which the Fifth Circuit rejected, is a transparent and impermissible attempt to resurrect their right to appeal the issuance of the Preliminary Injunction which they already waived. In their desperate attempt to avoid complying with the Preliminary Injunction, Defendants have resorted to revisionist history and misrepresentations of the record to bizarrely claim that, although they may have conspired to hack a computer which contained Konnech data, it may not have been a Konnech-owned computer that was hacked. Defendants’ superficial Motion is belied by their pre-suit and in-court statements admitting to gaining unauthorized access to a Konnech computer and taking the personal identifying information of millions of U.S. poll workers. Defendants’ Motion to Dissolve should be denied.

First, Defendants failed to identify any significant changed facts or circumstances to warrant dissolving the Preliminary Injunction. The Preliminary Injunction was not issued *ex parte*, but rather after full briefing and an oral hearing. Defendants had ample opportunity to present evidence as to why the Preliminary Injunction should not issue, but they chose not to. Instead, Defendants relied solely on argument of counsel—just as they do here—which is simply not evidence. Defendants also failed to appeal the Preliminary Injunction within 30 days as permitted by 28 U.S.C. § 1292(a)(1), even after the Fifth Circuit reminded Defendants of their right to do so. Instead, on the date of the appeal deadline, Defendants filed a mandamus petition with the Fifth Circuit—the wrong procedural mechanism—which was quickly rejected. Apparently realizing their error, and *after* their deadline to appeal, Defendants filed the underlying Motion to Dissolve

the same day that the Fifth Circuit rejected their mandamus petition. Indeed, Defendants’ Motion to Dissolve is a virtual carbon copy of their rejected mandamus petition even in the manner in which they address this Court as the Fifth Circuit. Defendants’ Motion to Dissolve should be denied, because it does not present any evidence to demonstrate *any* change in fact or law—let alone a “significant change” that is required for the dissolution of a preliminary injunction. Moreover, the claimed “novel” legal issues raised by Defendants in their Motion to Dissolve were already briefed in their Response to Konnech’s Motion for Preliminary Injunction. There are simply no changed facts or circumstances to warrant dissolving the Preliminary Injunction that Defendants chose not to appeal.

Second, Defendants’ own pre-suit statements—which were properly submitted as evidence by Konnech and considered by the Court in ruling on the Preliminary Injunction—admit that the server in question was a Konnech computer. Indeed, in explaining whose computer Defendants and their co-conspirators breached, Defendants specifically referred to Konnech by name, referred to the tradename of the software it owns (i.e., “PollChief”), and otherwise referred to the location of Konnech’s offices. Full transcripts of these podcasts were submitted with Konnech’s Motion for Preliminary Injunction for the Court’s consideration. Defendants cannot otherwise hide from their own in-Court testimony where they further admitted that the server at issue was a Konnech computer. The Preliminary Injunction is therefore supported by Defendants admission that they hacked into a Konnech computer and took the personal identifying information of millions of U.S. poll workers.

Third, the Preliminary Injunction properly issued because Konnech met its burden to show a substantial likelihood of success on the merits, irreparable harm to Konnech that outweighs any harm to Defendants, and that the Preliminary Injunction is in the public’s interest.

The Court should deny Defendants' Motion to Dissolve.

BACKGROUND

On September 12, 2022, Konnech filed suit against Defendants claiming, among other things, violation of the federal Computer Fraud and Abuse Act, 18 U.S.C. § 1030, *et. seq.*, and the Texas Harmful Access by Computer Statute, Tex. Civ. Prac. & Rem. Code § 143.001. (Doc. 1). That same day, Konnech filed a Motion for Temporary Restraining Order and Preliminary Injunction and Brief in Support (the "Motion for Preliminary Injunction"). (Doc. 5). As evidence in support of Konnech's Motion for Preliminary Injunction, Konnech attached an affidavit of its CEO, Eugene Yu which, among other things, proved up several podcasts in which Defendants repeatedly and publicly admitted to hacking into a Konnech computer and taking data therefrom, including the personal identifying information of an alleged 1.8 million U.S. poll workers. (Doc. 5-1). The Court issued an *ex parte* TRO based on such evidence. (Doc. 9).

On October 5, 2022, the day before the hearing on Konnech's Motion for Preliminary Injunction, Defendants filed their Opposition, which did not include any evidence in support of their opposition, and which did not otherwise object to the evidence submitted with Konnech's Motion for Preliminary Injunction. (Doc. 24). Instead, relying purely on argument of counsel, that opposition addressed the same arguments as Defendants' Motion to Dissolve, including their argument about the "Truth About Konnech" document, as well as their meritless argument that using a default password does not constitute hacking. (*Id.*).

On October 6, 2022, the Court held a hearing on Konnech's Motion for Preliminary Injunction. Defendants could have appeared at the hearing and provided testimony to support their arguments against the Preliminary Injunction, but they chose not to. On October 11, 2022, Konnech filed its Reply in Support of its Motion for Preliminary Injunction. (Doc. 27).

Accordingly, after full briefing from the Parties and after a hearing on October 6, the Court issued a Preliminary Injunction on October 31, 2022 which ordered that Defendants, their agents and assigns: (1) not access or attempt to access Konnech's computers; (2) not use or exploit the data taken from Konnech's computers; (3) identify each individual and/or organization involved in accessing Konnech's computers; (4) return to Konnech all data obtained from its computers; (5) preserve any data obtained from Konnech's computers; (6) disclose to Konnech how, when and by whom its computers were accessed; and (7) identify all persons and/or entities who have had possession, custody or control of any information or data from Konnech's computers. (Doc. 57).

As the Court explained in its Memorandum Opinion and Order, "[t]his data, whether acquired from Konnech or China, is personal and confidential to Konnech and the poll workers of the various counties and States in the United States where the workers are employed." (*Id.* at p. 6). As such, "[i]n accessing Konnech's computer and/or collecting, storing or retrieving data known to belong to Konnech, the defendants have interfered with Konnech's lawful right to control its own computers and data, and, moreover, protect the personal and confidential data of individuals who serve as 'poll workers.'" (*Id.* at p. 7). And furthermore, as the Court explained, "Konnech and Yu are under threats as a result of the defendants' media events, whereby they announced their intent to release to the public all of the data that they acquired from Konnech's protected computers. To do so, in the Court's opinion, would destroy trust in the governmental entities by the public and, trust between the governmental entities and Konnech." (*Id.*).

The Court also found Defendants in contempt of the *ex parte* TRO at an October 27, 2022 hearing, and on October 31, 2022, Defendants were detained pending their compliance with that TRO. (Doc. 51). Defendants, however, obtained an emergency order to release them pending review of a petition for mandamus. In the interim, on November 14, 2022, Defendants filed an

answer without moving to dismiss any of Konnech's claims under Rule 12(b)(6), thereby waiving their right to do so. (Doc. 60).

On November 22, 2022, the Fifth Circuit granted Defendants' Petition for Mandamus related to the Court's contempt finding for violation of the TRO (Konnech has since filed a Petition for *En Banc* Rehearing which is still being considered by the Fifth Circuit). In the Fifth Circuit's opinion, the panel did not address the validity of the Preliminary Injunction but reminded Defendants of their right to appeal the Preliminary Injunction, and advised them of their 30-day deadline to do so under 28 U.S.C. § 1292(a)(1) and FED. R. APP. P. 4(a)(1)(A). Accordingly, Defendants' deadline to file a notice of appeal for the Preliminary Injunction was November 30, 2022 or 30 days after the Preliminary Injunction was issued.

However, Defendants did not appeal the Preliminary Injunction. Instead, on November 30, they filed another petition for mandamus with the Fifth Circuit—the wrong procedural mechanism—and it was swiftly rejected. (Ex. B, Letter from Fifth Circuit Rejecting Filing). Realizing their error, and knowing that they were passed their deadline to file an appeal, on December 1, 2022, Defendants filed the instant Motion to Dissolve.¹ (Doc. 65).

The Motion to Dissolve is a duplicate of the Petition for Mandamus that was filed and rejected by the Fifth Circuit, and even refers to the Parties as "Petitioners" and "Respondents," and refers to this Court as the "District Court" and the "lower court." And notably, the Motion to Dissolve is riddled with objectively false statements about the record and the evidence presented to the Court.

¹ Defendants apparently filed three separate versions of the Motion to Dissolve, but the latest version is docketed as ECF Document 65.

The Motion to Dissolve also is replete with not-so-thinly veiled attacks on the Court. As one example, Defendants state in the Motion to Dissolve claims that the Court did not examine the record before issuing the Preliminary Injunction. (Mot. at p. 4) (“It [the Court] should have examined the record itself.”). As another example, Defendants stated that the Court denied Defendants procedural and substantive due process because the Court was “motivated by political side-taking[.]” (Mot. at p. 4). Defendants also accuse the Court of “gloss[ing] over” and “not so much as paus[ing] to address” the arguments previously briefed. (Mot. at p. 10). Defendants further falsely accuse the Court of dereliction of its duties by not reviewing the evidence submitted by Konnech in support of its Motion for Preliminary Injunction. (Mot. at p. 17) (“The district court could have readily consulted the podcasts offered as the sole basis for federal jurisdiction[.]”).

On December 5, 2022, Konnech filed a Motion to Show Cause and For Contempt Against Defendants Related to the Preliminary Injunction and Direct Orders from the Bench. (Doc. 67) As demonstrated therein, Defendants have not complied with the Preliminary Injunction in the nearly two months since it has been issued. In fact, Defendant Phillips admitted his contempt in an affidavit filed after the October 27 show cause hearing when he swore that he would comply with Sections 1-4 of the TRO (which are sections i, ii, iv, and v of the Preliminary Injunction), and “with all diligence, expedience, and in good faith,” provide the information required by Section 6 of the TRO (which is section vi of the Preliminary Injunction). (Doc. 46). But it has been nearly two months since that affidavit was filed, and Defendants have made no effort to comply.

Regardless, Defendants are attempting to use this Motion to Dissolve as a means to resurrect their long since waived appeal. But aside from their legally impermissible tactics, the Motion to Dissolve raises no new changes in law or fact, and should be denied.

ARGUMENT

A. Defendants Have Not Identified Any Significant Change of Fact or Law

Defendants have not demonstrated any change of fact or law since the Preliminary Injunction issued, let alone the “significant” change required to dissolve the Preliminary Injunction. Rather, Defendants seek to dissolve the Preliminary Injunction for the sole impermissible purpose of resetting their deadline to appeal which they already waived.

The United States Supreme Court has determined that Federal Rule 60(b)(5) applies to motions to dissolve preliminary injunctions and that it is appropriate to do so only where there exists “a significant change either in factual conditions or in law[.]” *Total Safety v. Knox*, 4:19-CV-02719. 2019 WL 6894683, at *2 (S.D. Tex. Dec. 18, 2019) (citing and quoting *Horne v. Flores*, 557 U.S. 433, 477 (2009)); *Bear Ranch, L.L.C. v. Heartbrand Beef, Inc.*, 885 F.3d 794, 803 (5th Cir. 2018) (refusing to find district court abused its discretion by denying motion to modify injunction where there was “no showing of a significant change in circumstances.”); *ICEE Distributors, Inc. v. J&J Snack Foods Corp.*, 445 F.3d 841, 850 (5th Cir. 2006) (“Modification of an injunction is appropriate when the legal or factual circumstances justifying the injunction have changed.”); *MILLC v. Fpusa, LLC*, No. SA:15-CV-406-DAE, 2016 WL 6088344, at *3 (W.D. Tex. Oct. 17, 2016) (“Ordinarily, the purpose of a motion to modify an injunction is to demonstrate that changed circumstances make the continuation of the order inequitable.”); *Ahmad v. City of St. Louis*, 995 F.3d 635, 640 (8th Cir. 2021) (“Modifying or dissolving a preliminary injunction is proper only when there has been a change of circumstances[.]”) (quoting *Favia v. Indiana Univ. of Penn.*, 7 F.3d 332, 337 (3d Cir. 1993)). When there is a change, the change raised by the movant cannot be simply *any* change. *Total Safety*, 2019 WL 6894683 at *2. Rather, the change must be a “significant change.” *Id.*; see *Bear Ranch*, 885 F.3d at 803 (basing decision on the lack of a “significant change”).

Defendants’ Motion to Dissolve does not identify any change in the facts or the law whatsoever, let alone a significant change. Furthermore, Defendants have not presented any evidence, let alone new evidence, to demonstrate any changes circumstances. Instead, Defendants’ Motion is premised on the notion that the Court is “confused,” misunderstands the facts, or did not even consider the facts that the Court had before it when it issued the Preliminary Injunction. (Doc. 65 at p. 2). If any of that were true, which it is not, Defendants should have appealed.

If a motion to dissolve was not based on changed circumstances, a party could “regain its lost opportunity” to appeal a preliminary injunction pursuant to 28 U.S.C. § 1292(a)(1) “simply by making a motion to modify or dissolve the injunction, having the motion denied, and appealing the denial.” *Karnoski v. Trump*, 926 F.3d 1180, 1198 (9th Cir. 2019); *see Alto v. Black*, 738 F.3d 1111, 1120 (9th Cir. 2013) (the requirement of a change in circumstances “presumes that the moving party could have appealed the grant of the injunction but chose not to do so, and thus that a subsequent challenge to the injunctive relief must rest on grounds that could not have been raised before.”); *Favia*, 7 F. 3d at 337-38 (“When a district court enters an order granting preliminary injunctive relief, parties who take exception to its terms must either file a motion for reconsideration in the district court . . . under Rule 59(e), bring an interlocutory appeal from that order under 28 U.S.C.A. § 1292(a)(1), or wait until the preliminary injunction becomes final and then appeal.”); *Lichtenberg v. Besicorp Grp. Inc.*, 204 F.3d 397, 401 (2d Cir. 2000) (same).

Because Defendants have not raised any significant change in law or facts, and because Defendants failed to timely appeal the Preliminary Injunction, Defendants are attempting to use this Motion to Dissolve as a backdoor to an appeal they already waived. *See Franklin Twp. V. Sewerage Auth. V. Middlesex Cnty. v. Utilities Auth.*, 787 F.2d 117, 121 (3d Cir. 1986) (“Now that the time for appeal has run, Woodbridge may not avoid the consequences of its failure to appeal

timely by cloaking its late appeal in the guise of a motion to dissolve the injunction.”). This is impermissible, and Defendants have no right to a second bite at the proverbial apple. *Ahmad*, 995 F.3d at 646 (“Even though the City captioned its motion as a request to ‘dissolve’ the injunction, the essence of its motion was a request to reconsider the injunction. That the City relied on evidence existing before the district court entered the preliminary injunction is fatal and should have ended the inquiry[.]”).

Defendants’ Motion to Dissolve should be denied because they have failed to show any significant change in law or fact.

B. Defendants Produced No Evidence To Support Dissolving the Preliminary Injunction

Defendants have not produced any evidence in support of their Motion to Dissolve and they cannot therefore meet their heavy evidentiary burden.

When seeking to dissolve a preliminary injunction, “[t]he party seeking relief bears the burden of establishing that the change in circumstances warrants the relief.” *Total Safety*, 2019 WL 6894683 at *2. “In persuading the court to dissolve a preliminary injunction, the moving party must make a strong evidentiary showing.” *Fiber Sys. Int’l, Inc. v. Applied Optical Sys., Inc.*, No. 2:06-CV-473, 2009 WL 8590962, at *2 (E.D. Tex. June 24, 2009) (citing *United States v. Swift & Co.*, 286 U.S. 106 (1932)). But here, Defendants have put forth *zero* evidence just as they failed to do in their response in opposition to Konnech’s Motion for Preliminary Injunction. (Doc. 24). Defendants’ counsel also attended a hearing on Konnech’s Motion for Preliminary Injunction but, again, Defendants chose not to appear and testify, and they otherwise failed to present any evidence to oppose the motion. (Ex. C, Oct. 6 Hrg. Tr. at 43:23-25). Defendants’ Motion to Dissolve again relies solely on argument of counsel which is not evidence and is insufficient to meet their heavy evidentiary burden. And although, objectively speaking, Defendants falsely assert that their

testimony from the October 27 hearing is “the only actual evidence presented to the district court by either party,” they do not even cite to it. (Mot. at p. 16).

Defendants’ failure to put forth any evidence fails to meet their burden of making a “strong evidentiary showing,” and their Motion to Dissolve should be denied.

C. The Preliminary Injunction is Valid and Should Not Be Dissolved

The Court issued a valid Preliminary Injunction and Defendants should remain enjoined pending a resolution of Konnech’s claims on the merits.

Defendants repeatedly and publicly admitted to hacking, or otherwise conspiring to hack into Konnech’s computers and taking its data. (Doc. 5, 5-1). Contrary to Defendants’ objectively false claims in their Motion to Dissolve, the Preliminary Injunction was issued based on Defendants’ pre-suit admissions which were properly submitted as evidence (and Defendants have never objected to the evidence either). (*Id.*). Defendants, however, now claim that the Court was confused about those statements. (Mot. at p. 2). Specifically, Defendants claim that their public statements were only about accessing a “Chinese server,” not a Konnech computer. (*Id.* at pp. 2-3). But Defendants’ argument is nothing more than a mischaracterization of their own statements and an exercise in revisionist history.

The Preliminary Injunction was based, in part², on Defendants’ alleged violation of the CFAA, which prohibits unauthorized access to a “protected computer” for purposes of obtaining information, causing damage, or perpetrating fraud. *Quantab Techs. Ltd. v. Golevsky*, 719 F. Supp. 2d 766, 775 (S.D. Tex. 2010); 18 U.S.C. § 1030, *et. seq.* The CFAA defines a computer as “an electronic, magnetic, optical, electrochemical, or other high speed data processing device

² Defendants glaringly fail to challenge the Texas state hacking statute on which the Preliminary Injunction also issued, i.e., TEXAS CIVIL PRACTICE AND REMEDIES CODE § 143.001. The Court should deny Defendants’ Motion to Dissolve on that basis alone.

performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device[.]” 18 U.S.C. § 1030(e)(1). The term “protected computer” is further defined to include “a computer . . . which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.” 18 U.S.C. § 1030(e)(2)(B-C). In other words, the term “protected computer” plainly includes a computer server or database located anywhere in the world if it is connected to the internet. *See Heil Trailer Int’l, Co. v. Kula*, No. 4:12-cv-385-Y, 2012 WL 12877645, at *1 (N.D. Tex. Aug. 21, 2012) (“If a computer system is connected to the internet, it qualifies as a protected computer under the CFAA[.]”).

A claim under Section 18 U.S.C. § 1030(a)(2)(c)³ of the CFAA has four elements: (1) a defendant intentionally accessed a protected computer; (2) without authorization or exceeding authorized access; (3) the defendant obtained information; and (4) the plaintiff suffered damage or loss of at least \$5,000. *See Florida Atlantic Univ. Bd. of Trustees v. Parsont*, 465 F. Supp. 3d 1279, 1289 (S.D. Fla. 2020). Defendants do not deny they obtained information from a protected

³ Defendants belatedly attempt to argue that Konnech somehow didn’t plead a claim under the CFAA by arguing that Konnech’s Complaint is “vague about stating which provision of the CFAA” Defendants violated. (Mot. at p. 8). In doing so, Defendants impermissibly seek to have a Motion to Dismiss under FRCP 12(b)(6) heard after they answered without filing such a motion. Konnech objects to Defendants’ attempt to have a FRCP 12(b)(6) motion to dismiss heard after they missed their deadline to file it. Further, Defendants’ Motion does nothing but demonstrate their misunderstanding of the CFAA or, otherwise, their failure to read the statute in its entirety. For example, Defendants point to Konnech’s Complaint which mentions a \$5,000 threshold that Defendants claim is only connected to Section 1030(a)(4), which relates to fraud claims, and then further points out that Konnech’s Complaint does not plead fraud. (Mot. at pp. 8-9). But Defendants apparently failed to read Section 1030(g), which creates a requirement of \$5,000 in damages or losses to maintain any civil action under the CFAA (which is also a criminal statute). In other words, Section 1030(g) requires that any civil complainant who sues under the CFAA, including Section 1030(a)(2)(c)—not just 1030(a)(4)—must have suffered \$5,000 in losses or damages within a 1-year period. 18 U.S.C. § 1030(g).

computer, nor otherwise deny that Konnech suffered damages or loss of at least \$5,000. Rather, Defendants argue that Konnech did not show a likelihood of success on the merits because Defendants claim they did not access a Konnech-owned computer, and that a novel question of law—which they fail to acknowledge was fully briefed to the Court before it issued the Preliminary Injunction—somehow precluded the Court from issuing the Preliminary Injunction. Defendants are wrong on both accounts.

1. Konnech Demonstrated a Substantial Likelihood of Success on the Merits

i. Defendants Publicly Claimed to Hacking Konnech’s Computers

Defendants cannot avoid the sum and substance of their repeated and public admissions that the computer they claimed to have accessed without authorization and taking data therefrom was a Konnech computer despite their hollow claims of cherry-picked quotes.

For example, on the September 2, 2022 Patriot Games podcast, which was submitted as Exhibit A-3 in support of Konnech’s Motion for Preliminary Injunction, Defendants specifically refer to Konnech by name when discussing the Chinese server they claimed to have hacked: “One of the first things that really came to us was that this data from this company, and these apps **apps.Konnech.com is one of the one of the URLs lives in China**, it lives on the main Unicom backbone in China.” (Doc. 5 at Ex. A-3 at p. 3) (emphasis added). To remedy any potential confusion about which Konnech they could be referring to, Defendants made sure to clarify that they were referring to a “company that was running the election management software, the company is based in Michigan, just outside of Lansing.” (*Id.*) Konnech, of course is an election management software company based outside of Lansing, Michigan. (Doc. 1 at ¶ 12; Doc. 5-1 at ¶ 2). Defendants were clearly referring to breaching a Konnech “computer,” as that term is defined under the CFAA.

Similarly, on September 8, 2022, Defendant Phillips ReTruthed an article which quoted him from another August 2022 podcast, during which he claimed that by using BinaryEdge, Defendants “learned in our review, **apps.konnech.com [.net], resolved into this same URL in China, meaning that the application itself was residing in China.**”⁴ (Doc. 1 at ¶ 37) (emphasis added). Further, Defendant Phillips claimed that, “[i]n BinaryEdge, you can figure out what type of database they are using, their database port, and all the different services offered by ports in this particular application living in China. It turned out that not only did it live there, but they left the database open.”⁵ The database, Defendant Phillips claimed, “stored the personal identifying information of over a million Americans.”⁶ Of course, not only did Defendant Phillips specifically refer to a Konnech URL by name, but the personal identifying information allegedly found on a Chinese server is clearly the same information Defendants claimed to have taken from Konnech.

As another example, during the August 30, 2022 podcast submitted as Exhibit A-2 in support of Konnech’s Motion for Preliminary Injunction, Defendant Phillips attempted to explain what he and his co-conspirators⁷ did with respect to hacking Konnech’s computers. (Doc. 5 at Ex. A-2). On that podcast, Defendant Phillips refers to “PollChief,” a trademarked software run exclusively by Konnech, when discussing that he found the “US based company” had “apps” that “were running from China, the database is running in China.” (*Id.*). To further ensure that his listeners understood he was discussing Konnech without explicitly saying so, Phillips claimed that

⁴ See KanekoaTheGreat, *FBI Conceals Chinese Infiltration of U.S. Election Software*, Kanekoa News (Sept. 8, 2022), available at <https://kanekoa.substack.com/p/fbi-conceals-chinese-infiltration>.

⁵ *Id.*

⁶ *Id.*

⁷ Defendants’ argument that Defendant Phillips could be the only defendant potentially liable for hacking (Mot. at pp. 7-8) ignores that Defendant Engelbrecht admitted to conspiracy when she stated that she and True the Vote “pulled in [Defendant Phillips’] team, and asked them to take a deeper dive” around the security of Konnech’s software.” (Doc. 5 at Ex. A-3).

this was “an app, run by a company based in Michigan[.]” (*Id.*). Defendant Phillips also told listeners that BinaryEdge showed a “particular IP address” for “this company [that] created a software that manages elections,” and that BinaryEdge “not only tells you what URLs resolved there . . . but it tells you where it lives. Where does this server live? And you can actually track it down and you track it down to China. . . on the main Unicom backbone in China.” (*Id.*). Again, it is undisputed that Konnech is an election logistics management company based out of Michigan that owns the software PollChief. (Doc. 1 at ¶ 12; Doc. 5-1 at ¶ 2). There is no question that Defendant Phillips was referring to a Konnech application and URL that he claims was running on a server in China—again, meeting the definition of “computer” under the CFAA. *See* 18 U.S.C. § 1030(e)(1) (defining “computer” to include “storage function” and “any data storage facility or communications facility directly related to or operating in conjunction with such device[.]”).

And as a further example of Defendants’ pre-suit statements admitting to hacking a Konnech computer, on the August 23, 2022 podcast submitted as Exhibit A-1 in support of Konnech’s Motion for Preliminary Injunction, Defendant Phillips discussed his January 2021 hotel room rendezvous and explained how his guys “showed [him] the database, they showed [him] where it lived. And it lives on the main, the main backbone, the Unicom backbone in China.” (Doc. 5 at Ex. A-1). When asked by the podcast host “who gave China all of this information? I mean, how did this even happen?” Defendant Phillips answered “there’s a company in the US based . . . just outside of Lansing, Michigan, and actually they operated an office in Lansing, run by a former Chinese national[.]” (*Id.*). Again, Defendant Phillips was clearly referring to a Konnech database which he said was living on the Chinese Unicom backbone.

Defendants continued their confession of liability by way of sworn, in-court testimony. At the October 27 Show Cause Hearing, Defendant Phillips again acknowledged that he understood

the computer from which he was shown poll worker data was a Konnech computer: “Q. Do you know anything about where he got the data that he showed to you in that hotel room? A. He told me that he accessed it from a server in China. Q. Did he mention the name ‘Konnech’ in that regard? A. Not directly, but it was indirectly related because of the way he showed me where the server was.” (Ex. A, Oct. 27 Hrg. Tr. at 46:9-17). Even more to the point, Defendant Phillips admitted that the server he and his co-conspirators accessed was in fact a Konnech computer: “**Q. Was there anything on that data that you saw that indicated it came from Konnech? A. Well, it came from an IP address that the URL that they were accessing it through resolved to. Yes. Q. Was there anything on the data itself that said ‘Konnech’? A. Yes.**” (*Id.* at 59:5-11) (emphasis added). And furthermore, when asked to identify who had possession of any data “from a Konnech protected computer,” Defendant Phillips answered “Mike Hasson,” one of his co-conspirators. (*Id.* at 71:22-72:1).

Defendant Engelbrecht likewise confirmed her understanding that the computer from which the poll worker data was accessed was a Konnech computer when testifying: “BinaryEdge indicates that there are many Konnech-run websites that resolve in China” (*id.* at 134:12-13) and, moreover, that “**Konnech is hosting all of their data in China.**” (*Id.* at 134:19-20) (emphasis added); *see* 18 U.S.C. § 1030(e)(1) (defining “computer” to include “storage function” and “any data storage facility or communications facility directly related to or operating in conjunction with such device[.]”). Accordingly, there is no dispute that Defendants claimed to have hacked into a Konnech computer, and their desperate attempt to distinguish between a Konnech computer and a “Chinese server” is meritless.

Moreover, Defendants’ reliance on the “Truth About Konnech” document (which is not evidence) in an attempt to avoid liability for their admitted hacking is baseless. (Mot. at pp. 13-

15). Defendants make light of Konnech’s “Truth About Konnech” document which resulted from Defendants’ attacks on Konnech and which was created to address Konnech’s customers’ concerns resulting from such attacks. (Doc. 24 at pp. 1, 5, 9-11). In that document, Konnech specifically said that it found no breach of its system after conducting an internal investigation. But that doesn’t mean a breach didn’t happen, especially given Defendants’ repeated public statements bragging about breaching a Konnech computer and taking Konnech’s private data. (Doc. 5 at Exs. A-1, A-2, A-3, A-4).

Defendants’ argument, in essence, is that simply because Konnech’s internal investigation was unable to identify how Defendants breached their servers, they are exonerated. To be clear, the “Truth About Konnech” document does *not* say that Konnech was not hacked, as Defendants characterize it. Rather, it merely says that Konnech was unable to find evidence of a breach on its system. Using the “breaking and entering” analogy used by federal courts when analyzing hacking claims under the CFAA, Defendants would have this Court believe they should be exonerated merely because a homeowner was unable to find evidence that their home was broken into, all while the criminal publicly confesses to his unlawful activity. *See HiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180, 1194-202 (9th Cir. 2022) (explaining that the legislative history of the CFAA reflects that “the conduct that is prohibited is analogous to that of ‘breaking and entering’” and the court should “therefore look to whether the conduct at issue is analogous to ‘breaking and entering.’”).

Defendants’ other argument, that they could not have hacked into a Konnech computer because Konnech says it does not store any data in China, is irrelevant. Aside from the fact that the Truth About Konnech document is not evidence nor submitted with any sworn statement, the fact of the matter is Defendants have admitted to accessing a Konnech computer, without

authorization, and taking data therefrom. Whether Defendants are lying, or perhaps confused themselves, about the location of the computer they hacked into is an entirely separate matter that will be used to demonstrate Defendants' defamation. But **Defendants cannot avoid the Preliminary Injunction when they have admitted to hacking a Konnech computer and taking its data, regardless of its geographic location.** (Ex. A, Oct. 27 Hrg. Tr. at 59:5-11) ("Q. Was there anything on that data that you saw that indicated it came from Konnech? A. Well, it came from an IP address that the URL that they were accessing it through resolved to. Yes. Q. Was there anything on the data itself that said 'Konnech'? A. Yes.").

Defendants also take issue with the quotes Konnech included in its Original Complaint—not the Motion for Preliminary Injunction—claiming that they were somehow improperly “cherry-pick[ed]” and that “it is clear Phillips is talking about a server in China.” (Mot. at p. 6). As an initial matter, a digital copy of each podcast and a full copy of each podcast transcript was submitted to the Court for consideration in connection with Konnech's Motion for Preliminary Injunction. (Doc. 5-1). In other words, Konnech provided the Court with copies of the entire podcasts and transcripts with the Motion for Preliminary Injunction. (*Id.*)

In any event, Defendants' own cherry-picking misstates the substance of those podcasts. For example, though Defendants state that “Phillips never mentioned Konnech in the quoted podcast segments” of its Original Complaint (Mot. at p.5), as shown above, Defendant Phillips specifically mentioned Konnech by name on the September 2, 2022 Patriot Games podcast, which was submitted as Exhibit A-3 in support of Konnech's Motion for Preliminary Injunction. (Doc. 5-1 at Ex. A-3) (“One of the first things that really came to us was that this data from this company, and these apps apps.Konnech.com is one of the one of the URLs lives in China, it lives on the main Unicom backbone in China.”). Moreover, as shown above in this section, and as is apparent from

the sum and substance of each podcast, in every instance that Defendants referred to a “Chinese server” or the “Chinese internet,” they were always speaking about a Konnech computer. (Doc. 5-1 at Exs. A-1, A-2, A-3). Defendants cannot now backtrack and distance themselves from their admitted misconduct by somehow drawing a false distinction between a computer in China and a Konnech computer, particularly where their own in-court testimony confirms that they were always discussing a Konnech computer. (Ex. A, Oct. 27 Hrg. Tr. at 59:5-11) (“Q. Was there anything on that data that you saw that indicated it came from Konnech? A. Well, it came from an IP address that the URL that they were accessing it through resolved to. Yes. Q. Was there anything on the data itself that said ‘Konnech’? A. Yes.”). Again, regardless of the geographic location of the Konnech computer, and prior to the issuance of the Preliminary Injunction, Defendants admitted to accessing a Konnech computer without authorization and taking its data. (*Id.*).

ii. Using a Password Without Authorization to Access a Computer Constitutes Hacking

Defendants again misstate the record by accusing the Court of “gloss[ing] over” what Defendants contend is a “novel question of law” concerning whether Defendants’ admitted access to a Konnech computer using a default password was “without authorization.” (Mot. at p. 10). To be clear, despite the fact that the Parties briefed this very issue—indeed, Defendants cite to and quote the exact same cases they previously addressed in the Parties’ original briefing—Defendants accuse this Court of failing to consider it: “But whether access is ‘without authorization’ or ‘exceeds’ what is authorized is a complex legal and factual question *that the district court did no so much as pause to address.*”⁸ (Mot. at p. 10) (emphasis added). But aside from Defendants’

⁸ Far from failing to consider Defendants’ repeated argument as to whether use of a default password constitutes hacking, the Court specifically questioned Defendants about the use of a default password at the October 27 show cause hearing (*see e.g.*, Ex. A, Oct. 27 Hrg. Tr. at 94:9-

objectively false statements about the record⁹, Defendants' use of a password without authorization constitutes hacking under the CFAA.

In *Florida Atlantic University Bd. of Trustees v. Parson*, the court issued a preliminary injunction based on the CFAA where the defendant, who was not a current student at the university, used passwords provided to him by current students to access the University's network. 465 F. Supp. 3d at 1287. In other words, the court found that, like here, even though Defendants claim that they merely used a password made available to them, the unauthorized use of that password which allowed access to a protected computer constituted a violation of the CFAA. *Id.*

Similarly, in *U.S. v. Nosal II*, a former employee used a current employee's password to access his former employers' protected computer. 844 F.3d 1024, 1038 (9th Cir. 2016). The court found that a showing that a party circumvents technological barriers is not necessary to prove that a party accessed a computer without authorization under the CFAA. *Id.* at 1032. Rather, all that is necessary is that a party used a password without authorization. *Id.*

And in *HiQ Labs* a case which Defendants again rely on in a futile effort to avoid liability (but which actually demonstrates that what Defendants admit to having done is unlawful), the court was tasked with addressing the meaning of "without authorization" as used in the CFAA. 31 F.4th at 1194-202. There, the court determined that the term "without authorization" is "analogous to

95:6), and further acknowledged Defendants' argument in the Preliminary Injunction memorandum opinion and order. (Doc. 57) (addressing Defendants' arguments, including that "Konnech's pleadings, affidavit, and exhibits fail to demonstrate that its computers were hacked," and further noting that "except for taking issue with whether they 'hacked' Konnech's computers, they do not deny the assertions in Yu's affidavit.").

⁹ Defendants also falsely state that Defendant Phillips was "the only person in the room during any arguable 'access'," (Mot. at p. 9) despite specifically testifying that there was a third, unnamed individual who was in the room, which was the basis of Defendants' contempt in the first place. (Ex. A, Oct. 27 Hrg. Tr. at 41:1-5).

‘breaking and entering.’” *Id.* at 1197. The *hiQ* court thus distinguished between public LinkedIn profiles, wherein one can access data contained thereon without any password, and a website which contains some sort of restriction or authorization requirement, such as a password. *Id.* (“[T]he prohibition on unauthorized access is properly understood to apply only to private information—information delineated as private through use of a permission requirement of some sort.”). As such, “[w]ith regards to websites made freely accessible on the Internet, the ‘breaking and entering’ analogue . . . has no application, and the concept of ‘without authorization’ is inapt.” *Id.* at 1198.¹⁰

Unlike the data at issue in *hiQ*,¹¹ the data Defendants claimed to have taken was indeed private and, in fact, it was admittedly restricted by a password which should have been a red flag to Defendants that the information was intended to be protected as private. (Doc. 24 at p. 8). As Mr. Yu testified, Defendants had never been given authorization to use that password or to take that private data from a Konnech server. (See Doc. 5 at Exs. A at ¶ 5). Using the “breaking and entering analogy” addressed by the *hiQ* court, what Defendants claimed to have done is no different than breaking and entering into Konnech’s offices by using a key accidentally left in the front door.

¹⁰ Defendants also reference *Van Buren v. United States*, 141 S. Ct. 1648 (2021) in their Motion to Dissolve. (Mot. at p. 10). But *Van Buren* is entirely inapplicable. There, the Court merely held that there was no violation of the CFAA where an individual had authorization to access a protected computer, but had an improper motive for doing so. *Id.* at 1662. But here, Defendants have never been authorized or granted permission to access any non-public Konnech protected computer. (Mot. Ex. A at ¶ 5).

¹¹ The court explained that “[t]he data *hiQ* seeks to access is not owned by LinkedIn and has not been demarcated by LinkedIn as private using such an authorization system.” *Id.* at 1201.

2. Konnech Demonstrated Threats of Immediate and Irreparable Harm

The Preliminary Injunction was also issued based on evidence that Konnech will suffer immediate and irreparable harm absent the injunction. Specifically, Konnech submitted evidence that it would suffer immediate and irreparable harm by: (a) the unauthorized access to Konnech's protected computers; (b) the unauthorized use and/or disclosure of data from Konnech's protected computers; (c) interference with Konnech's control of its protected computers; (d) breach of security of Konnech's protected computers; (e) disclosure of confidential information contained on Konnech's protected computers; and (f) loss of confidence and trust of Konnech's customers, loss of goodwill, and loss of business reputation. (Doc. 5 at Ex. A). Defendants never submitted any evidence in response to the Motion.

Courts have uniformly held that mere interference with an entity's control of its computer systems constitutes irreparable injury. *See FAU Bd. of Trustees*, 465 F. Supp. 3d at 1296 (“Unsurprisingly, federal courts around the country agree that the interference with an entity's control of its computer systems constitutes irreparable injury.”); *Facebook, Inc. v. Power Ventures, Inc.*, 252 F. Supp. 3d 765, 782 (N.D. Cal. 2017), *aff'd*, 749 F. App'x 557 (9th Cir. 2019) (“[I]n accessing [the plaintiffs] computers without authorization, Defendants have interfered with [the plaintiffs] right to control access to its own computers and have acquired data to which Defendants have no lawful right in violation of the CFAA,” thus causing irreparable injury); *Reliable Prop. Servs., LLC v. Capital Growth Partners, LLC*, 1 F. Supp. 3d 961, 965 (D. Minn. 2014) (finding “substantial threat of irreparable harm” based on the public dissemination of information after the defendant “unlawfully took volumes of detailed data” in violation of the CFAA); *Enargy Power Co. v. Xiaolong Wang*, No. 13-11348-DJC, 2013 WL 6234625, at *10 (D. Mass. Dec. 3, 2013) (“[P]revent[ing] Enargy from enjoying the uninterrupted use of its property . . . constitutes irreparable harm.”). Consistent with prior decisions, the Court here likewise found that “[i]n

accessing Konnech’s computer and/or collecting, storing or retrieving data known to belong to Konnech, the defendants have interfered with Konnech’s lawful right to control its own computers and data, and, moreover, protect the personal and confidential data of individuals who serve as ‘poll workers.’” (Doc. 57).

Konnech also demonstrated that failing to enjoin Defendants will lead to loss of confidence and trust of Konnech’s customers, and loss of Konnech’s goodwill and business reputation. *See Mach 1, LLC v. Adaptisoft, LLC*, No. SA-21-CV-00114-XR, 2021 WL 6750834, at *2 (W.D. Tex. Feb. 16, 2021) (finding irreparable injury in connection with CFAA violation where business “reputation will suffer as unreliable in an area where reliability is very important.”); *Fletcher’s Original State Fair Corny Dogs, LLC v. Fletcher-Warner Holdings LLC*, 434 F. Supp. 3d 473, 496 (E.D. Tex. 2020) (“Grounds for irreparable injury include loss of control of reputation, loss of trade, and loss of goodwill.”). The Court also found this to be a concern, and addressed those concerns in its memorandum opinion. (Doc. 57) (“To do so, in the Court’s opinion, would destroy trust in the governmental entities by the public and, trust between the governmental entities and Konnech.”).

Konnech further demonstrated that the disclosure of the personal identifying information Defendants claimed to have taken from Konnech will cause irreparable harm and would constitute a clearly unwarranted invasion of personal privacy. (Doc. 5, 5-1 at ¶ 7); *see* TEX. BUS. & COMM. CODE § 521 (protecting personal identifying information); *see also U.S. Dept. of Defense v. Federal Labor Relations Authority*, 510 U.S. 487, 502 (1994) (holding that nondisclosure of “home addresses substantially outweighs the negligible FOIA-related public interest in disclosure” and “would constitute a ‘clearly unwarranted invasion of personal privacy.’”); *Lamb v. Millennium Challenge Corp.*, 334 F. Supp. 3d 204, 214-15 (D. D.C. 2018) (“Generally, personal identifying

information such as a person's . . . social security number may be protected under Exemption 6" of FOIA). Again, the Court agreed with these concerns. (Doc. 57) ("This data . . . is personal and confidential to Konnech and the poll workers of the various counties and states in the United States where the workers are employed.").

Accordingly, Konnech demonstrated imminent irreparable harm and the Preliminary Injunction was therefore properly issued.

3. Konnech Demonstrated that the Balance of Hardships Weighs in Konnech's Favor

Konnech also demonstrated that the balance of hardships upon the issuance of a preliminary injunction weighs decidedly in Konnech's favor. As numerous courts have held, when a defendant, such as Defendants here, engages in unlawful conduct prohibited by state or federal law, the Court need not consider hardship to the defendant. *See FAU Bd. of Trustees*, 465 F. Supp. 3d at 1297; *see also MediaOne of Delaware, Inc. v. E & A Beepers & Cellulares*, 43 F. Supp. 2d 1348, 1354 (S.D. Fla. 1998) (explaining that a defendant suffers no hardship when an injunction "will merely enjoin [the defendant] from conducting a business which is already prohibited by state and federal law"); *accord YourNetDating, Inc. v. Mitchell*, 88 F. Supp. 2d 870, 872 (N.D. Ill. 2000) (explaining the defendants "will suffer no legitimate harm of which they can complain if the [injunctive relief] is granted because they have no honest business hacking [the plaintiff's] system[.]"). The Preliminary Injunction is necessary for Konnech to secure its data and prevent the continued theft of the data. (Doc. 5 at ¶ 7).

The injunction interferes only with Defendants' unlawful access of Konnech's protected computers, without any interruption to Defendants' legitimate business (if any). *See FAU Bd. of Trustees*, 465 F. Supp. 3d at 1297 ("Here, the balance weighs decidedly in FAU's favor. On the one hand, if an injunction does not issue, FAU will face 'significant harm to the security of its

systems and data, theft of its secured, proprietary, and/or confidential information and systems, and privacy dangers to its students.”). Nevertheless, Defendants claim that they “have already been harmed by the TRO and injunction” because “they were held in contempt and confined in jail for a week[.]” (Mot. at p. 18). But the harm Defendants complain of is self-inflicted. Defendants would never have been confined if they would have simply complied with the TRO, including identifying all persons involved in accessing Konnech’s computers during that January 2021 hotel meeting.

To be clear, although Defendants characterize certain requirements of the Preliminary Injunction as improper “premature discovery,” (Mot. at p. 2) all aspects of the Preliminary Injunction are vital to maintaining the status quo and protecting Konnech’s computers and the data stored thereon. Specifically, it is necessary to immediately obtain the identities of all persons involved so that they too can be restrained before causing further irreparable harm before it’s too late. (Doc. 5, 5-1). It is also necessary to immediately know how Konnech’s computers were accessed so that any alleged security flaw can be remedied before any more of its data is stolen. (*Id.*) And moreover, it is necessary to immediately know who all possessed the data so that they can be restrained before publicly releasing it. (*Id.*) Accordingly, the Preliminary Injunction is designed to maintain the status quo by preventing harm to Konnech and the data it maintains.¹²

¹² Even if sections iii, vi, and vii of the Preliminary Injunction could be considered “early discovery,” the preliminary injunction is proper. Specifically, a mandatory preliminary injunction may be issued “upon a strong showing of necessity and upon equitable grounds which are clearly apparent.” *Fox v. City of West Palm Beach*, 383 F.2d 189, 194 (5th Cir. 1967) (“[W]here the necessity exists and the grounds are shown courts will not hesitate in granting the remedy” of mandatory injunctive relief). Konnech has, of course, met that burden given the need to protect the improper access and disclosure of the personal identifying information of 1.8 million U.S. poll workers.

4. Konnech Demonstrated that the Preliminary Injunction is in the Public's Interest

Both the Texas Harmful Access by Computer statute and the CFAA are criminal statutes which provide for a private civil action, and, therefore, the public interest is advanced by enforcing compliance with the laws of Texas and the United States. *See FAU Bd. of Trustees*, 465 F. Supp. 3d at 1298. In other words, “[s]ince the injunction does nothing more than prevent conduct that Congress has already deemed criminal, it necessarily advances the public interest.” *Id.* Additionally, courts have routinely held that the “public has an interest in ensuring that computers are not accessed without authorization.” *Facebook, Inc.*, 252 F. Supp. 3d at 785.

Moreover, the injunction implicates the privacy rights and interests of Konnech’s customers and allegedly 1.8 million U.S. poll workers. *See FAU Bd. of Trustees*, 465 F. Supp. 3d at 1298 (finding injunction in the public’s interest where defendant’s unauthorized access of FAU’s protected computer implicated the privacy rights of FAU students). In fact, it is paramount that the Court maintain the injunction to secure the integrity of poll worker’s personal identifying information, which Defendants have admitted is a serious matter and should not be publicly disclosed. (Ex. A, Oct. 27 Hrg. Tr. at 153:2-15); (Doc. 57) (explaining that Defendants’ conduct has “interfered with Konnech’s lawful right to . . . protect the personal and confidential data of individuals,”; and that such conduct is “to the detriment of . . . the governmental entities and their employees.”).

The Preliminary Injunction was properly issued and it should not be dissolved.¹³

¹³ Defendants’ proposed order appears to inadvertently state that “the *TRO* and preliminary injunction . . . must be dissolved.” However, the *TRO* was already dissolved upon the issuance of the Preliminary Injunction. (Docs. 18, 20, 57).

PRAYER

Konnech, Inc. respectfully requests that the Court deny Defendants' motion to dissolve preliminary injunction, and grant Konnech, Inc. for such other and further relief to which it may be justly entitled.

Dated: December 22, 2022

KASOWITZ BENSON TORRES LLP

By: /s/ Constantine Z. Pamphilis
Constantine Z. Pamphilis
Attorney in Charge
Texas State Bar No. 00794419
SDTX Bar No. 19378
DPamphilis@kasowitz.com
Nathan W. Richardson
Texas State Bar No. 24094914
SDTX Bar No. 24094914
NRichardson@kasowitz.com
1415 Louisiana Street, Suite 2100
Houston, Texas 77002
(713) 220-8800
(713) 222-0843 (fax)

Attorneys for Plaintiff Konnech, Inc.

CERTIFICATE OF SERVICE

I hereby certify that on December 22, 2022, true and correct copies of the above and foregoing were forwarded via email and through the ECF system, to all parties and counsel of record.

/s/ Constantine Z. Pamphilis
Constantine Z. Pamphilis

Exhibit A

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF TEXAS

- - -

THE HONORABLE KENNETH M. HOYT, JUDGE PRESIDING

KONNECH, INC.,) Cause No. 4:22-cv-03096
)
Plaintiff,)
)
vs.)
)
TRUE THE VOTE, et al.,)
)
Defendants.)
)

HEARING

OFFICIAL COURT REPORTER'S TRANSCRIPT

Houston, Texas

October 27, 2022

APPEARANCES:

On behalf of the Plaintiff:

Constantine Z. Pamphilis, Esq.

Nathan Richardson, Esq.

On behalf of the Defendants:

Brock Cordt Akers, Esq. (Not present)

Michael John Wynne, Esq

John C. Kiyonaga, Esq.

Reported By: Nichole Forrest, CSR, RDR, CRR, CRC
Certified Realtime Reporter
United States District Court
Southern District of Texas

Proceedings recorded by mechanical stenography.
Transcript produced by Reporter on computer.

| | | |
|----|-------------------------------------|------|
| 1 | EXAMINATION INDEX | |
| 2 | WITNESSES | PAGE |
| 3 | GREGG PHILLIPS | |
| 4 | Direct Examination By Mr. Wynne | 29 |
| 5 | Cross-Examination By Mr. Pamphilis | 37 |
| 6 | CATHERINE ENGELBRECHT | |
| 7 | Direct Examination By Mr. Wynne | 106 |
| 8 | Cross-Examination By Mr. Richardson | 109 |
| 9 | Redirect Examination By Mr. Wynne | 166 |
| 10 | | |
| 11 | | |
| 12 | | |
| 13 | | |
| 14 | | |
| 15 | | |
| 16 | | |
| 17 | | |
| 18 | | |
| 19 | | |
| 20 | | |
| 21 | | |
| 22 | | |
| 23 | | |
| 24 | | |
| 25 | | |

1 Q. Was there anybody, other than you,
2 Mr. Hasson, and this confidential informant, as you
3 say, that you won't identify, in that hotel room that
4 night?

5 A. No.

6 Q. What's your relationship with this other
7 individual that was there?

8 A. He was a contractor.

9 Q. He was a contractor for you?

10 A. Yes.

11 Q. Was he someone that you paid to be there?

12 A. Yes -- no, not to be there, but he was a
13 contractor.

14 Q. Did you have a contractual relationship with
15 him?

16 A. Earlier in 2020, yes.

17 Q. What was the nature of the contractual
18 relationship?

19 A. Advised me.

20 Q. On what sort of matters?

21 A. Matters about election intelligence.

22 Q. Is he the one who arranged this meeting
23 between you and Mr. Hasson in that hotel room in
24 January of 2021?

25 A. I don't know. I don't think so.

1 A. It might be.

2 Q. Did you have that information when you went
3 to meet with Mr. Hasson in January of 2021 that he was
4 a confidential informant, as you were told?

5 A. I think so.

6 Q. Did you have reason to believe that
7 Mr. Hasson was someone that you could trust?

8 A. Sure.

9 Q. Do you know anything about where he got the
10 data that he showed to you in that hotel room?

11 A. He told me that he accessed it from a server
12 in China.

13 Q. Did he mention the name "Konnech" in that
14 regard?

15 A. Not directly, but it was indirectly related
16 because of the way that he showed me where the server
17 was.

18 Q. Were you able to independently verify that
19 that data you were seeing came from a Konnech server
20 in China?

21 A. Was I able to? No, but that's not my job.
22 My job was to -- once I learned it, to hand off the
23 information to the FBI.

24 Q. Your job for who?

25 A. The FBI, as a confidential informant.

1 A. I don't know.

2 Q. Did you actually look at the data when you
3 were in that hotel room?

4 A. Yes.

5 Q. Was there anything on the data that you saw
6 that indicated it came from Konnech?

7 A. Well, it came from an IP address that the URL
8 that they were accessing it through resolved to. Yes.

9 Q. Was there anything on the data itself that
10 said "Konnech"?

11 A. Yes.

12 Q. Not the URL. That said it on the data you
13 were looking at?

14 A. There was all sorts of folders and things
15 that were being accessed. So, sure.

16 Q. And how many -- you characterized it before
17 as poll worker records. Is that what it was?

18 A. It's the tip of the iceberg, but that was
19 some of it, yeah.

20 Q. How many poll worker records were there?

21 A. There were 1.8 million records in that
22 particular system. But it wasn't just -- the way that
23 they configure everything, it wasn't just poll
24 workers. It was election judges. There was all sorts
25 of entries for the equipment; different software they

1 Q. We haven't heard from someone who is actually
2 an employee or agent of True The Vote, have we?

3 A. I think as a contractor, I'm an agent. But
4 I'm not a lawyer. So I don't know.

5 Q. You're not an employee of True The Vote, are
6 you?

7 A. No.

8 Q. Not an officer or director, are you?

9 A. No, sir.

10 Q. Catherine Engelbrecht is the president of
11 that company, isn't she?

12 A. Yes.

13 Q. We haven't heard from her, have we?

14 A. She wasn't there.

15 Q. That wasn't my question.

16 We haven't heard from her on this?

17 A. I don't know.

18 Q. You've been in the courtroom all day. Have
19 you heard her get on the stand and testify?

20 Have you?

21 A. No.

22 Q. For section 7: "Identify all persons and
23 entities in your knowledge who had possession of any
24 data from a Konnech protected computer."

25 Who do you identify?

1 A. Mike Hasson and the FBI.

2 Q. And even though you saw it, you don't think
3 that you ever had possession of it?

4 A. No, sir.

5 Q. Even though you saw it for four-and-a-half
6 hours?

7 A. Yes, sir.

8 Q. And are you in a position to say whether the
9 L.A. County D.A. ever had it?

10 A. This data? No, sir.

11 Q. Did the L.A. D.A. show you what data they do
12 have?

13 A. No, sir.

14 Q. Did you ever see an evidence receipt from the
15 FBI for this data that Mike Hasson allegedly provided
16 to them?

17 A. No.

18 Q. Did you ever ask for one?

19 A. No.

20 Q. But you're working with them as a
21 confidential informant; right?

22 A. Yes.

23 Q. These same people that you say got the data;
24 right?

25 A. Yes.

1 around and trying to find things. But we also do
2 geospatial research.

3 THE COURT: Were you planning to put the
4 names of the individuals who worked for the Harris
5 County polling, Bexar County polling, all of that data
6 that you said that you saw, were you planning to post
7 that data on a public venue?

8 THE WITNESS: No, sir.

9 THE COURT: Does this sound familiar to
10 you: Gregg and Catherine, GC -- that's you, Gregg and
11 Catherine -- stumbled onto voting software used to
12 corroborate elections. Was left with default
13 password.

14 What is a default password?

15 THE WITNESS: A password that the software
16 would be shipped with.

17 THE COURT: Is what?

18 THE WITNESS: When they ship it to be
19 installed.

20 THE COURT: That means that someone has
21 intercepted a password?

22 THE WITNESS: No, sir. It ships with the
23 password. I think that is what it's referring to.

24 THE COURT: No. I'm asking you what
25 you're referring to.

1 It says here: You were left with -- you
2 used to coordinate the elections, was left with
3 default password of database.

4 What are you talking about?

5 THE WITNESS: Like I said, a password that
6 would be shipped with the software.

7 THE COURT: And so the software you're
8 referring to is what?

9 THE WITNESS: I don't recall. I mean,
10 do --

11 THE COURT: We're talking about this
12 software. We're talking about this data.

13 THE WITNESS: Well, I don't know that we
14 are or aren't. We could be talking about the
15 Open.INK.

16 THE COURT: But you're the one talking
17 about it.

18 THE WITNESS: Right. But I don't know if
19 that's what I was referring to.

20 THE COURT: Well, you said you stumbled
21 onto voting software used to coordinate elections.

22 That is what Konnech does, isn't it?

23 THE WITNESS: I think it's one of the
24 things they do.

25 THE COURT: Well, do they do it or not?

1 Chinese UNICOM backbone in China, according to
2 BinaryEdge.

3 MR. RICHARDSON: Objection.
4 Nonresponsive.

5 BY MR. RICHARDSON:

6 Q. I'm asking you about the security
7 vulnerabilities you just mentioned.

8 A. Okay.

9 Q. Do you know or do you not know actual
10 security vulnerabilities of any Konnech computer,
11 software, server or the like?

12 A. BinaryEdge indicates that there are many
13 Konnech-run websites that resolve in China. I guess I
14 don't understand the question.

15 Q. Security would mean -- a flaw in security,
16 something that makes it accessible --

17 A. You're right. Then that must be intentional.

18 Q. What is intentional?

19 A. That Konnech is hosting all of their data in
20 China.

21 MR. RICHARDSON: Objection.
22 Nonresponsive.

23 THE COURT: I'll sustain it.

24 BY MR. RICHARDSON:

25 Q. My question is: Do you know of any security

1 THE WITNESS: No, sir.

2 THE COURT: If that data had the names of
3 individuals who were poll workers in many counties
4 throughout the United States, personal information;
5 names, addresses Social Security numbers, bank account
6 numbers, that kind of information was what was
7 accessed, do you believe that that is a serious
8 matter?

9 THE WITNESS: Absolutely, yes.

10 THE COURT: And that's the kind of
11 information that you would not want --

12 THE WITNESS: No, sir.

13 THE COURT: -- public to disclose;
14 correct?

15 THE WITNESS: No, sir.

16 THE COURT: The way that you answered your
17 questions leaves me to believe, and you can correct
18 me, that True The Vote was under investigation by the
19 FBI involved because it was involved in some -- the DC
20 FBI involved, and felt that you were involved, you
21 meaning True The Vote was involved in some activity
22 that might violate federal law.

23 At some point in time this Konnech was
24 offered up by your company as a way of, I guess,
25 vindicating what you were doing, and they then

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

C E R T I F I C A T E

I hereby certify that pursuant to Title
28, Section 753 United States Code, the foregoing is a
true and correct transcript of the stenographically
reported proceedings in the above matter.

Certified on October 30, 2022.

/s/ Nichole Forrest
Nichole Forrest, RDR, CRR, CRC

Exhibit B

United States Court of Appeals

FIFTH CIRCUIT
OFFICE OF THE CLERK

LYLE W. CAYCE
CLERK

TEL. 504-310-7700
600 S. MAESTRI PLACE,
Suite 115
NEW ORLEANS, LA 70130

December 01, 2022

Mr. Michael Wynne
Gregor Wynne Arney, P.L.L.C.
909 Fannin Street
Suite 3800
Houston, TX 77010

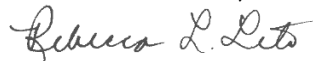
No. 22-20578 In re: Gregg Phillips
USDC No. 4:22-CV-3096

Dear Mr. Wynne,

We are in receipt of the document titled "Petition for Writ of Mandamus to Dissolve Temporary Injunction" filed on November 30, 2022, in the referenced appeal. Because this document must be filed as an original proceeding, it will be removed from the docket of this appeal.

Sincerely,

LYLE W. CAYCE, Clerk



By: _____
Rebecca L. Leto, Deputy Clerk
504-310-7703

cc: Mr. Constantine Z. Pamphilis

Exhibit C

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

KONNECH, INC., . 4:22-CV-03096
 . HOUSTON, TEXAS
 PLAINTIFF, . OCTOBER 6, 2022
VS. . 1:59 P.M.
 .
TRUE THE VOTE, INC., .
 .
GREGG PHILLIPS AND .
 .
CATHERINE ENGELBRECHT, .
 .
DEFENDANTS. .
.....

TRANSCRIPT OF PRELIMINARY INJUNCTION HEARING
BEFORE THE HONORABLE KENNETH M. HOYT
UNITED STATES DISTRICT JUDGE

APPEARANCES

FOR THE PLAINTIFF:

Constantine Z. Pamphilis
Nathan Richardson
KASOWITZ BENSON TORRES LLP
Wedge International Tower
1415 Louisiana
Suite 2100
Houston, Texas 77002

FOR THE DEFENDANTS:

Brock C. Akers
J. Mark Brewer
THE AKERS FIRM
3401 Allen Parkway
Suite 101
Houston, Texas 77019

APPEARANCES - CONTINUED

OFFICIAL COURT REPORTER:

Mayra Malone, CSR, RMR, CRR
U.S. Courthouse
515 Rusk
Room 8004
Houston, Texas 77002
713-250-5787

Proceedings recorded by mechanical stenography. Transcript
produced by computer-aided transcription.

1 THE COURT: Maybe I misread it. I apologize.
2 Apparently, I misread the letter or the communication.

3 There was a motion for show cause having to do
4 with the motion for contempt. How am I to proceed on that?
5 Your clients are going to have to be here.

6 MR. BREWER: Okay.

7 THE COURT: So I can enter an order ordering them to
8 be here. We can have a hearing and decide at that point
9 whether or not -- maybe plaintiff has got this all wrong.

10 MR. BREWER: Your Honor, respectfully, we don't need a
11 show cause order. If you want to set a hearing, an evidentiary
12 hearing --

13 THE COURT: They need a show cause hearing. I need a
14 show cause hearing. When they made allegations that someone
15 has violated my order, it is incumbent upon the Court to move
16 to bring the parties together to figure out if there's merit to
17 what the claim is, what the motion is.

18 MR. BREWER: Just to be clear, Your Honor, at no time
19 were we ever asked to bring any witnesses today. I just wanted
20 you to know, we are not -- we would have brought them, but we
21 didn't know that that was even an issue. We thought we were
22 here on the TRO.

23 THE COURT: Why didn't you bring your clients and
24 disprove their case then? They would have been able to get on
25 the witness stand and say, It ain't so, Judge. It ain't so.

1 submitted.

2 THE COURT: All right. I will not stand in the way of
3 lawyers filing responses or replies. He's filing a response.
4 You would be filing a reply to the response, and I'm saying
5 that I will not delay considering this matter waiting on a
6 reply. If you want to file it, that's fine.

7 MR. AKERS: Understood.

8 THE COURT: Thank you, gentlemen.

9 MR. PAMPHILIS: Thank you, Your Honor.

10 *(Court adjourned at 3:10 PM)*

11 * * * *

12 I certify that the foregoing is a correct transcript from
13 the record of proceedings in the above-entitled cause.

14
15 Date: October 8, 2022

16 */s/ Mayra Malone*

17 -----
18 Mayra Malone, CSR, RMR, CRR
19 Official Court Reporter
20
21
22
23
24
25